VPN (VIRTUAL PRIVATE NETWORK) A SECURED WAY OF HANDLING DATA OVER NETWORK

by

Juttiyavar Mahesh N *

ABSTRACT

Describes about Virtual Private Network [VPN] and its use in libraries for secured way of transferring information and data to their members. Also talks about its advantages and present status of VPN implementation at MASTEK.

Keywords: CAS-Web based PUSH Technology, CAS

---

* Sr. Executive Information Repository, Mastek Ltd., SDF VII, SEEPZ Andheri (E), MUMBAI

0   INTRODUCTION

The Internet has revolutionized internal and external business communications and processes offering ubiquitous, anytime-and-anywhere connectivity. In this decentralized business model that has evolved, it is now essential to interconnect not only corporate offices, but also remote and mobile employees who need access to the same applications used traditionally in offices. Organizations also need to communicate externally with business partners, suppliers, and customers to help form better relationships, reduce customer turnover, and streamline internal business processes. With their ability to bring together remote users and share ideas instantaneously, Internet VPNs have become an integral and critical element in achieving long-term business success. By all these changes and to leverage the benefit of flexible and available network, libraries are working towards implementing new technologies, VPN is one among them.

When people think of accessing library information from outside the library, they tend to think of free access through the Internet. There are lots of libraries such as corporate, medical, and law, however, that need to limit access to their information. Even public libraries have information that they make available only to specific groups (employees, volunteers, etc.). How are these libraries to limit access to their information and ensure only the appropriate people access the appropriate information? The answer is 'Virtual Private Networks', popularly known as VPN.

1   WHAT IS VPN?

A Virtual Private Network is a private data network that makes use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN acts as a direct secure connection between clients i.e., a private one. A Virtual private network can be considered as a system of owned or leased lines that can be used by only one corporate body. It allows remote users to access the library servers, connect a library site, and be the underlying security architecture for extranets.

VPN doesn't require a dedicated line, anyone with Internet access can use this. Users can be given access to everything on the network that they would normally use in the library. VPN contains security features that make hijacking data or gaining improper access to the WAN very difficult. The idea of VPN is to give any corporate body a private network at much lower cost by using shared public infrastructure rather than a private one.

According to University of Rochester Information Technology website (http://www.rochester.edu/its/telecom/vpn/)VPN is a system through which you can connect to University of Rochester resources from home as if you were on campus. This allows you access to resources, which are restricted because of security or copyright issues, such as pop3 access to University mail servers and access to many library databases.
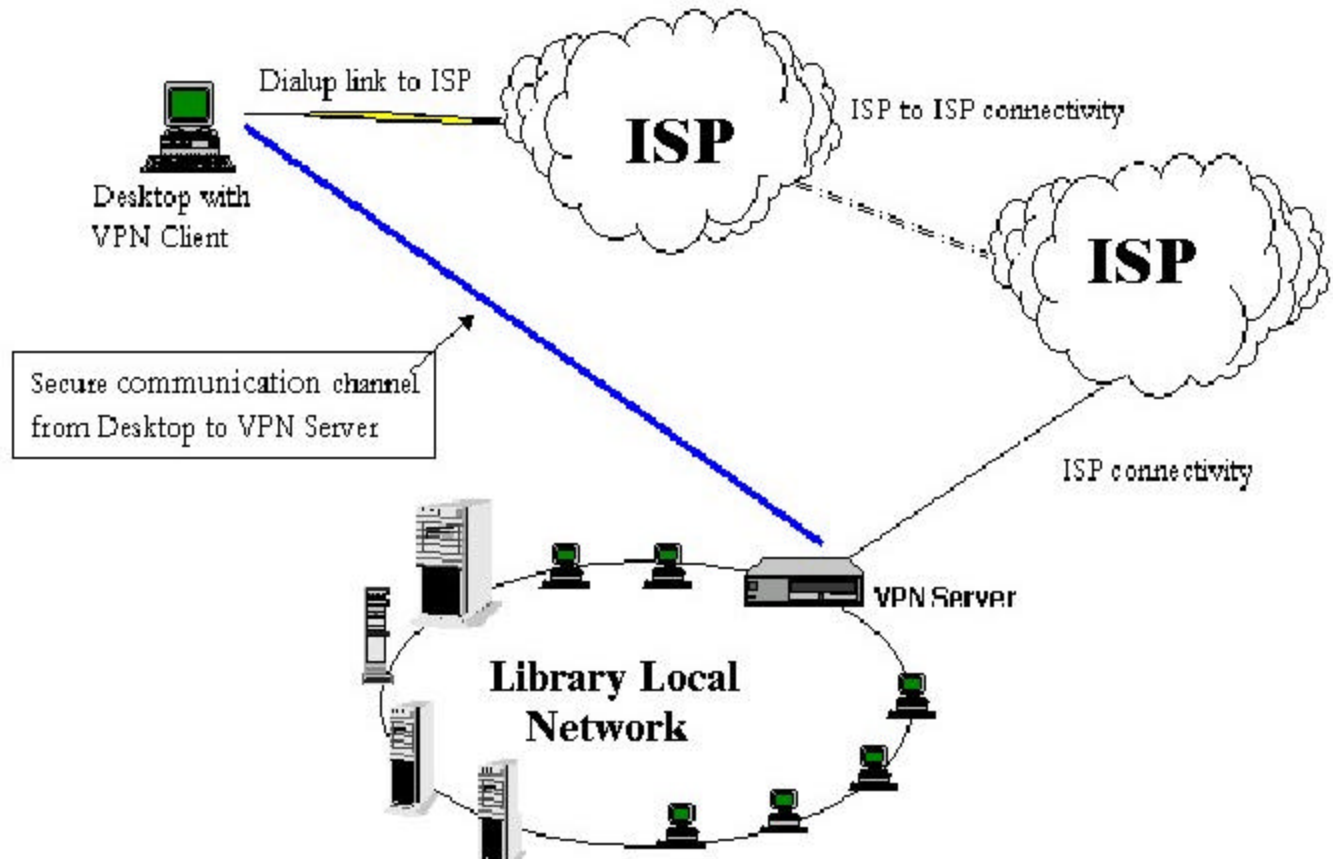
1.1   Connectivity

The VPN requires a software at both ends that encrypts outbound traffic and decrypts inbound. The software may run on dedicated hardware appliances or on a pc with a general-purpose operation system such as Linux, Netware or windows.

1.2   How does it work?

VPN allow users working at home or on the road to connect in a secure fashion to a remote server using the Internet. VPN technology also allows a main library to connect to its branch libraries or to other libraries over the Internet while maintaining secured communications. VPN involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. VPN software is typically installed as a part of organizations firewall server. VPN can use the Internet or the service provider's private frame relay, or asynchronous transfer mode (ATM) infrastructure. Typically a user will dial into an ISP like VSNL, to get connected to the Internet. After a successful connection, user will invoke VPN connection from a VPN client, which is configured on his/her machine.

VPN Setup

Dialup link to ISP

ISP

ISP to ISP connectivity

Desktop with
VPN Client

ISP

Secure communication channel
from Desktop to VPN Server

ISP connectivity

VPN Server

Library Local
Network

1.3   Advantages of VPN

The libraries can utilize VPN, as researchers are continually becoming less reliant on the physical library to conduct research. Bibliographic research can easily be conducted on-line. Many electronic databases are accessed through web interfaces. On-line texts from magazines are common. More and more libraries are investing in electronic resources. These libraries could easily provide their information over VPNs for their employees.

VPN represents the latest alternative for constructing a WAN to connect offices, Libraries, organizations and can address some networking problems more effectively and inexpensively compared to traditional WAN solutions such as frame relay and leased lines.
The following are some of the advantages of implementing VPN in an organization
- ?? **Cost effective solutions for site-to-site and remote access communication.**
- ?? **Global accessibility to business partners and others**
- ?? **Connectivity for Telecommuters, mobile users**
- ?? **Highly scalable, secured & flexible network**
- ?? **Email Via POP3**
- ?? **File access from remote places**

- ?? **Web based management**
- ?? **Arms employees with up-to-date information, enabling them to make timely, informed decisions**
- ?? **Extend the workplace beyond the office walls allowing employees to be fully productive at home and the road**
- ?? **Provide an edge in recruiting employees looking for flexible work styles such as telecommuting and job sharing**
- ?? **Establishes a complete competitive advantage by creating closer links with customer, supplier and employees**

2 Libraries using VPN Technology

Following libraries have already implemented VPN technology.
1. **The University of Hong Kong Digital Libraries Hong Kong (http://www.hku.hk/lib/)**
2. **The University of Rochester Library (http://www.lib.rochester.edu/database/)**
3. **Northwestern University Library, U.S.A (http://er.library.northwestern.edu/)**
4. **The University of Texas Southwestern Medical Center U.S.A (http://www3.utsouthwestern.edu/library/indexIE.htm)**
5. **Marshall School of Business, University of Southern California U.S.A. (http://www.marshall.usc.edu/web/Library.cfm?doc_id=2013)**
6. **IVE Libraries (http://www.vtc.edu.hk/lib/EleRes/EleRes_OffCampusAccess.htm)**
7. **Boston College, Chestnut Hill, MA (http://www.bc.edu/bc_org/avp/ulib/ref/remote.html)**

3 Solution at Mastek

To provide Mastekeers with the ability to connect to corporate computing resources, regardless of their location, we have implemented the PGP 300 e-ppliance, a Gauntlet based solution from Network Associates. E-ppliance 300 is an integrated hardware and software device that combines three security products in one—Gauntlet Firewall, Gauntlet VPN, and McAfee virus scan. Gauntlet Firewall works at all layers of network and regulates both inbound and outbound packets providing control over security. It is also capable of handling http throughput of up to 80 megabits per second. Gauntlet VPN encrypts, authenticates, and creates secure VPN tunnels across public networks. It uses strong cryptography of 3 DES to protect confidential data and works on open standards to ensure secure interoperability between different vendor solutions.

4 Conclusion

Here an effort has been made to describe Virtual Private Network (VPN) based on our initial stages of implementation at MASTEK. This also explains the use of VPN in libraries for secure ways of transferring the data and information.

5 Acknowledgements

6   REFERENCES

1. DUKE (J). VPNs: poised to take off. Business Communications Review; 29, p 40-42; June 1999.
2. KORZENIOWSKI (P). VPNs become key part of enterprise networks.
   Business Communications Review. 30, 3; 2000. p 28-32.
3. http://www.corecom.com/html/vpn.html
4. http://www.lic.gov.uk/publications/policyreports/building/tg16.html
5. http://www.rochester.edu/its/telecom/vpn/
6. http://www.techguide.com.
7. http://www.zdnet.com/devhead/resources/headsup/archive/000119.html